IMS-U PIA

1. Contact Information

> **A/GIS/IPS Director**
>
> Bureau of Administration
> Global Information Services
> Office of Information Programs and Services

2. System Information

(a) Name of system: Investigative Management System – Unclassified

(b) Bureau: Diplomatic Security (DS)

(c) System acronym: IMS-U

(d) iMatrix Asset ID Number: 799

(e) Reason for performing PIA: Click here to enter text.

☐ New system

☒ Significant modification to an existing system

☐ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable): The modification of the IMS-U System includes: (1) replacing the Oracle 10G Application Server with the Pivotal vFabric Suite 5.2, (2) upgrading the MS Biz Talk server operating system from Windows Server 2008 to Windows Server 2008, R2, and (3) the addition of the Autonomy 10.X search tool and decommission of the existing Oracle search tool (4) Review and validation of the NIST SP 800-53, Revision 4 Security Controls.

3. General Information

  (a) Does the system have a completed and submitted Security Categorization Form (SCF)?
     ☒Yes
     ☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

  (b) What is the security Assessment and Authorization (A&A) status of the system?
     The current version of IMS-U is 01.08.00, which has an authorization date through
     October 31, 2016. The system is currently undergoing a targeted Security Assessment
     (SA), which will increase the version number from 01.08.00 to 01.11.00.

  (c) Describe the purpose of the system:
     The Investigative Management System (IMS-U), Version (01.11.00) ITAB #(799)
     application supports the Diplomatic Security (DS) worldwide investigative mission by
     providing an enterprise-wide investigative case management system. The application
     captures all case related information, automates, integrates, and improves DS
     investigative business processes, establishes a central index encompassing all Diplomatic
     Security Service (DSS) investigations, provides investigative/intelligence analysis and
     analytical processing while creating internal and external electronic data sharing.

     IMS-U works with the Enterprise Case Assessment Service (ECAS), which is managed
     by the Bureau of Consular Affairs, Consular Systems and Technology (CA/CST). ECAS
     is a service module under the Consular Consolidated Database (CCD), iMatrix # 0009,
     which is an aggregate system comprised of a set of databases configured to hold all
     current and archived data from all databases that support Embassy, Post and Consulates
     around the world.

     ECAS is a tool that allows Fraud Prevention Units (FPUs) at overseas posts and Fraud
     Prevention Managers (FPMs) at domestic passport agencies and centers to track various
     types of consular fraud assessments. ECAS currently tracks visa, American Citizen
     Services (ACS), and domestic passport fraud. Suspected fraudulent information is sent to
     IMS-U via a Secure Socket Layer (SSL) protocol encrypted (https) connection and a
     Preliminary Inquiry (PQ) is opened. After suspected fraudulent information is reviewed
     in IMS-U, and it is determined that the individual suspected is indeed trying to do
     something illegal, then a field agent opens a case file and begins a documented
     investigation.

  (d) Describe the personally identifiable information (PII) that the system collects, uses,
     maintains, or disseminates:

     IMS collects and maintains the following types of PII on members of the public, foreign
     nationals, government employees, and contractors who are identified as being directly or
     indirectly involved in or associated with criminal allegations. All types of information
     may not be collected on each specific group of individuals. The IMS-U system processes
     the following types of PII:

- Full Birth Name (and any name/alias)
- Date and Place of Birth
- Social Security Number
- Driver's License Number
- Email addresses (home and business)
- Birth Certificate Number and corresponding information on parents from birth certificate
- Baptismal Records (This is legacy information imported from RAMS. This information is no longer collected. Seventy-four baptismal records are maintained by IMS).
- Addresses (home and business)
- Phone numbers (home and business)
- Biometric Information such as (gender, race, height, weight, eye color, skin tone, hair color, hair style, images, age or estimated age, body type (build), scar, marks, & tattoos
- Criminal History
- Citizenship status and Information (DSP-11 (Passport Application), OF-156 (VISA Application))
- Financial Account Numbers
- Medical Information
- Financial Information
- Legal Information
- Personnel Information
- Family Information

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

The legal authority for the collection of information is the same as that which established the Bureau of Diplomatic Security: The Omnibus Diplomatic Security and Antiterrorism Act of 1986 (Pub. L. 99-399; 22 U.S.C. 4801, et seq. (1986)) as amended. This legislation is cited in 12 Foreign Affairs Manual (FAM) 012, Legal Authorities.

Additional authorities are as follows:
- 26 Code of Federal Regulations (CFR) 601.017, Criminal Investigation Functions, April 1, 2007
- 22 U.S. Code 2709, Special Agents, January 3, 2012

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

☒Yes, provide:

- • SORN Name and Number: See below.
- • SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): See below.

   - STATE-31, Human Resources Records, July 19, 2013
   - STATE-36, Security Records, December 15, 2015
   - STATE-26, Passport Records, July 6, 2011
   - STATE-39, Visa Records, October 25, 2012

   ☐No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐Yes   ☒No

   If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes   ☐No
   (If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)

   If yes provide:
   - • Schedule number (e.g., (XX-587-XX-XXX)): A-11-012-19a through A-11-012-19g
   - • Length of time the information is retained in the system: See below.
   - • Type of information retained in the system: NARA schedule information retained in the system can be found at this link and is provided below:
     [http://infoaccess.state.gov/recordsmgt/recdispsched.asp?cat=records#domestic]

A-11-012-19a	**Investigative Management System (IMS)**
Description:	a. Master File
	An electronic tracking system used to control and document criminal investigations. Information covers case background, case allegations, case documented interviews, evidence, surveillance videos/audio tapes, pictures, post records and foreign government records, and related investigative information.
Disposition:	Temporary. Destroy/delete master file data 100 years after case closes. NOTE: If the Bureau of Diplomatic Security becomes aware of any significant or precedent-setting cases that may warrant preservation, notify NARA for an independent appraisal of these cases.
DispAuthNo:	N1-059-09-36, item 1a

A-11-012-19b   **Investigative Management System (IMS)**

Description: b. Input/Source Records

Hard copy (non-electronic) documents used to create, update, or modify electronic records when the electronic records are retained to meet recordkeeping requirements and are covered by a NARA-approved schedule. Included are such records as hard copy forms used for data input as well as hard copy documents that are scanned into an electronic recordkeeping system.

Disposition: Temporary. Destroy immediately after verification of successful conversion. (Supersedes GRS 20, item 2a[4]).

DispAuthNo: GRS 4.3, item 010

A-11-012-19c   **Investigative Management System (IMS)**

Description: c. Input/Source Records

Electronic records entered into the system during an update process, and not required for audit and legal purposes and electronic records received from other agencies.

Disposition: Temporary. Destroy immediately after data have been entered or otherwise incorporated into the master file or database and verified. (Supersedes GRS 20, item 2b).

DispAuthNo: GRS 4.3, item 020

A-11-012-19d   **Investigative Management System (IMS)**

Description: d. Outputs

Electronic files consisting solely of records extracted from a single master file or data base that is disposable under GRS 20 or approved for deletion by a NARA-approved disposition schedule, EXCLUDING extracts that are:
- Produced as disclosure-free files allow public access to the data; or

---

- Produced by an extraction process which changes the informational content of the source master file or data base; which may not be destroyed before security NARA approval.

Disposition: Temporary. Destroy when business use ceases. (Supersedes GRS 20, item 5).

DispAuthNo: GRS 4.3, item 031

A-11-012-19e   **Investigative Management System (IMS)**

Description: e. Outputs

Printouts derived from electronic records created on an ad hoc basis for reference purposes or to meet day-to-day business needs.

Disposition: Temporary. Destroy when business use ceases. (Supersedes GRS 20, item 16).

DispAuthNo: GRS 4.3, item 030

A-11-012-19f   **Investigative Management System (IMS)**

Description: f. Systems Backups

System Backups and Tape Library Records. Backup tapes maintained for potential system restoration in the event of a system failure or other unintentional loss of data.

Disposition: Temporary. Destroy when superseded by a full backup, or when no longer needed for system restoration, whichever is later. (Supersedes GRS 24, item 4a[1]).

DispAuthNo: GRS 3.2, item 040

A-11-012-19g   **Investigative Management System (IMS)**

Description: g. System Documentation

	Includes systems requirements, system design, and user guides.
Disposition:	Temporary. Destroy 5 years after the project/activity/transaction is completed or superseded, or the associated system is terminated, or the associated data is migrated to a successor system. (Supersedes GRS 20, item 11a[1]).
DispAuthNo:	GRS 3.1, item 051

- Passport and Visa File, Domestic Records Disposition Schedules Chapter 11: Diplomatic Security Records Office of Antiterrorism Assistance, Section A-11-008-06 - Files contain correspondence required in the process of applying for diplomatic and official passports and visas for staff personnel and contractors who perform tasks outside the U.S. Files include actual passports returned upon completion of task. Files arranged alphabetically by individual's name. Files span 2003 to present. Records are maintained for 5 years or upon separation of the bearer.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.
☒ Members of the Public
☒ U.S. Government employees/Contractor employees
☒ Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☒ Yes   ☐ No

- If yes, under what authorization?
The IMS-U system processes privacy data as defined by the Privacy Act of 1974. IMS-U contains PII data, including social security numbers. Additional information about the PII data elements is provided in question 3.d. above. Authorization for collecting SSNs for passport operations is 26 USC 6093E, and for Visa operations it is 8 USC 1182.

(c) How is the information collected?
The information collected by IMS-U is collected through direct input from interviews, uploading of documents or images, through web forms, via transfers from Consular Affairs Passport Lookout Tracking System (PLOTS) of identified fraud cases, through DS Law Enforcement investigative and analytical activities. All data is collected and entered/uploaded into the system by DS employees (i.e. Foreign Service and Civil Service Criminal Investigators, Intelligence Research Specialists, and DS employed contract investigators and Intelligence Research Specialists) as part of their official duties as a member of a Law Enforcement Organization (LEO). IMS-U receives information from the Enterprise Case Assessment Service (ECAS), which is a service module under

the Consular Consolidated Database (CCD). ECAS tracks visa, American Citizen Services (ACS), and domestic passport fraud. This information is sent to IMS-U in the event of suspected fraudulent information. IMS-U also receives data from the Diplomatic Security Evidence and Property System (DSEPS) application system. IMS-U receives Evidence Control File (ECF) information from DSEPS related to IMS-U cases.

(d) Where is the information housed?

☒ Department-owned equipment

☐ FEDRAMP-certified cloud

☐ Other Federal agency equipment or cloud

☐ Other

• If you did not select "Department-owned equipment," please specify.

N/A

(e) What process is used to determine if the information is accurate?

Assigned personnel validate data through cross-checking of disparate databases and through interviews. IMS-U has built-in data validation controls such as sequence checks, range checks, logical relationship checks, and validity checks. Sequence checks and range checks ensure that a control number follows sequentially and any out of sequence or duplicated control numbers are rejected prior to processing. The logical relationship check occurs if a particular condition is true, then one or more additional conditions or data input relationships may be required to be true to consider the input valid. Validity checks are programmed checking of the data validity in accordance with predetermined criteria. For example, an individual's biographical record contains a field for gender and the acceptable status codes are 'M' or 'F'. If any other code is entered the record will be rejected.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

The information is as current as the information received from the data sources. IMS-U personnel will have access to the system to manage data stored within the system database. This will ensure that data remains current if changes are needed. If by chance a case is opened within the IMS-U system to investigate fraudulent activities, users assigned functional roles have the ability to update cases with new information.

(g) Does the system use information from commercial sources? Is the information publicly available?

No. Open source data streams are only for those in the law enforcement community. Information is commercially provided, but not publically available.

(h) Is notice provided to the individual prior to the collection of his or her information?

The data for IMS-U is received from other applications; see the PIAs for the feeder systems for more information on how individuals receive notice.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☐Yes ☒No

- If yes, how do individuals grant consent?
- If no, why are individuals not allowed to provide consent?

Data for the IMS-U system is derived from other data sources, namely the PLOTS system, ECAS module, and DSEP system. Data received from these sources is not available to the public due to the nature of data, which is used to investigate fraudulent activities for passports, and visas. The system also processes law enforcement investigation data.

(j) How did privacy concerns influence the determination of what information would be collected by the system?

The collection of PII is limited to the required components of a criminal investigation. The only PII collected and retained is related to Passport Fraud (PF), Visa Fraud (VF), Regional Security Office, Protective Intelligence Investigations, Professional Responsibility and Criminal Investigative Liaison (CIL) cases that are collected in support of IMS-U investigations.

5. Use of information

(a) What is/are the intended use(s) for the information?

The IMS-U system allows DSS Office Special Agents and Intelligence Research Specialists as well as other authorized personnel to investigate and analyze data from headquarters, field offices and posts around the world. IMS-U affords centrally indexed, case tracking and management of information related to Passport Fraud (PF), Visa Fraud (VF), Regional Security Office, Protective Intelligence Investigations, Professional Responsibility, and Criminal Investigative Liaison (CIL) cases.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?
Yes. It was designed and developed for passport and visa fraud, and investigations.

(c) Does the system analyze the information stored in it? ☒Yes ☐No

If yes:
   (1) What types of methods are used to analyze the information?
   DS investigators and analysts are able to retrieve data based on text queries and then use the data to conduct criminal investigative analysis based on data collected and stored in IMS from various sources such as the DSP-11, OF-156, Motor Vehicle Records, LEO restricted databases (i.e. NCIC, TECS, etc.), and other outside sources. All DS case related data is maintained in the IMS system in order to provide a centrally indexed repository.

   (2) Does the analysis result in new information?

No new information on the record subject is produced.

(3) Will the new information be placed in the individual's record? ☐Yes   ☒No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? ☐Yes   ☒No

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

IMS-U receives data from three interface connections. The three interface connections are: 1) A bi-directional electronic interface connecting to Diplomatic Security Evidence and Property Systems (DSEPS) that is used to retrieve Evidence Control File (ECF) information related to investigative case information processed in IMS-U; 2) A one-way direct connection to Consular Consolidated Database (CCD) that is used to access investigative case information processed in the Enterprise Case Assessment Service (ECAS) module; and, 3) A one-way direct connection to the Passport Lookout Tracking System (PLOTS) application to allow agencies to track consular fraud assessments.

(b) What information will be shared?
The IMS-U system does not share information with other internal and/or external systems.
(c) What is the purpose for sharing the information?
N/A
(d) The information to be shared is transmitted or disclosed by what methods?
N/A
(e) What safeguards are in place for each internal or external sharing arrangement?
N/A
(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?
N/A

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?
As a law enforcement investigative system owned by the Bureau of Diplomatic Security, State SORN 36, 22 C.F.R. 171, permits IMS-U to be excluded from the access and redress provisions of the Privacy Act in order to prevent harm to law enforcement investigations or interests. However, access requests are considered under both the

Privacy Act and/or the Freedom of Information Act (FOIA) on a case-by-case basis if made under the procedures outlined in 22 C.F.R. Part 171.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.
To the extent that material contained in IMS-U is subject to the Privacy Act (5 USC 552a) individuals can request amendment of material in the system under procedures set forth in STATE 36. This amendment procedure is available only to information on non-criminal investigations. All information pertaining to criminal investigations is excluded from the Privacy Act under 5 USC 552a (j)(2). Inaccurate or erroneous information in criminal investigative files will only be subject to amendment or correction at the request of the federal law enforcement agency which originated the material.
If no, explain why not.

(c) By what means are individuals notified of the procedures to correct their information?
The mechanism for requesting correction of information is specified in State SORN 36, 22 C.F.R. Part 171, and this PIA.

8. Security Controls

(a) How is the information in the system secured?
Access controls are in place for the back-end Oracle database, which are based upon role-based permissions configured for "least privilege". The review process establishes segregation of duties for the application. Authentication to the application is established via windows authentication using single sign-on via OpenNet. Once a user logs into OpenNet and is authenticated, the end user is granted access to the IMS-U system. This is in place for a large majority of DS application systems.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.
Access to the IMS-U application is restricted to cleared DoS direct hire and contractor employees as addressed by a completed and approved Network Access Request (NAR) form. The application and database administrators are the only users with elevated privileged access to the database, and only for express purposes of troubleshooting and performing routine maintenance. Additionally, all access is enforced by user profiles according to the principle of least privilege and the concept of separation of duties. The Business Owner (DS/ICI/CR/CIR/VPAU) approves and authorizes use of the IMS-U system. System accounts are maintained and reviewed on a regular basis. The following DoS policies establish the requirements for access enforcement.

- 5 FAM 731 SYSTEM SECURITY (Department computer security policies apply to Web servers)

- 12 FAM 622.1-2 System Access Control
- 12 FAM 623.2-1 Access Controls
- 12 FAM 629.2-1 System Access Control
- 12 FAM 629.3-3 Access Controls

The database enforces a limit of 3 consecutive invalid access attempts by a user during a 15 minute time frame. After 20 minutes of inactivity a session lock control is implemented at the network layer.

The information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel. The level of access for the user restricts the data that may be seen and the degree to which data may be modified. A system use notification ("warning banner") is displayed before log-on is permitted, and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited. Non-production uses (e.g., testing, training) of production data are limited by administrative controls.

Diplomatic Security uses an array of configuration auditing and vulnerability scanning tools and techniques to periodically monitor the OpenNet-connected systems that host DS's major and minor applications, including the IMS-U components, for changes to the DoS mandated security controls.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?
IMS-U is monitored by inherited security controls of the OpenNet general support system. Controls built into OpenNet include routers and Network Intrusion Detection System (NIDS). These controls provide network level controls that limit the risk of unauthorized access from all IP segments, to include patch management, configuration management, and segregation of duties. In addition, the application is placed behind a virtual firewall to further limit access to system data.

(d) Explain the privacy training provided to authorized users of the system.
Department users are required to attend a security briefing before access to Department systems is granted. This briefing also includes privacy orientation. Users are also required to complete Cybersecurity Awareness Training on an annual basis and must acknowledge in place policies by signing user agreements. System administrators and privileged users are required to complete a separate security awareness briefing provided by the Information System Security Officer (ISSO) as well as sign an Acknowledgement of Understanding and Rules of Behavior statement.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes   ☐No
If yes, please explain.

Because PII is present in the application, FIPS 140-2 encryption is in place for all sessions. Users are only allowed access to data required for their particular task.

(f) How were the security measures above influenced by the type of information collected? The IMS-U application system is categorized as a "Moderate" risk system in accordance with FIPS 199. In light of this, NIST SP 800-53, Rev. 4 "Moderate" security controls were applied in accordance with OMB to ensure the security of the application as a whole, including the protection of PII.

9. Data Access

(a) Who has access to data in the system?
There are two groups of roles for the IMS-U system. They are descriptive roles and functional roles. For the descriptive roles, the following applies:
- o Every user has exactly one descriptive role.
- o A user's descriptive role is roughly equivalent to their job title.
- o No program logic depends on descriptive roles; they are merely cosmetic.

For the functional roles, the following applies:
- o Every user has zero or more functional roles.
- o Functional roles are used by IMS-U to enforce business rules and automatically perform actions (typically assignment).

(b) How is access to data in the system determined?
The business owner (DS/ICI/CR/CIR/VPAU) approves and authorizes access to the IMS-U system. Only authorized users have access to the IMS-U system.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes   ☐No

Procedural information can be found in documentation for the IMS-U system. This documentation is stored on the DS/CTO SharePoint site.

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

Access to IMS-U data is role based and configured within the Oracle 11G database. Least privilege and separation of duties are in place for the system. All users will not have access to all data in the system. PII is restricted to authorized personnel. Access is based upon least privilege controls configured for the IMS-U Oracle 11G database. Users are only allowed to access data required to complete particular tasks.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

Access controls are in place for the Oracle 11G databases. Access is based on role-based permissions configured for "least privilege", which establishes separation of duties (e.g. Cases are handled only by Special Agents). Authentication is established via Windows Authentication using single sign-on via the OpenNet general support system. Only database administrators have access to the IMS-U Oracle database.